CLAIMS

We Claim:

1. A method of windowed backward key generation, comprising:

a) providing information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series;

b) generating a key in the series, based at least in part on said information provided to said user;

c) providing said key in the series to the user; and

d) said user determining at least one key in the limited number of previous keys in the series by applying said information to said key in the series provided to the user.

2. The method of Claim 1, wherein said a) comprises providing a key rotation element that is forward rotatable by said user but is not backward rotatable.

3. The method of Claim 1, wherein said a) comprises providing to the user a key rotation exponent that is used to determine a previous key in the series from a later key in the series by exponentiating said later key by said key rotation exponent.

4. The method of Claim 2, further comprising:

e1) generating a new key rotation element;

e2) generating a new key based, in part, on said new key rotation element; and

e3) distributing said new key to non-revoked users.

5. The method of Claim 1, wherein said a) further comprises providing a secret share and a key rotation catalyst said user, wherein said secret share and said key rotation catalyst allow said user to generate a next key in the series provided sufficient public information is available.

6. The method of Claim 5, further comprising:

e) publishing at least one public share, wherein the next key in the series is determinable based on the key rotation catalyst, the secret share, and the at least one public share.

7. The method of Claim 5, further comprising revoking a user by publishing a version of the revoked user's secret share.

8. A method of windowed backward key rotation, comprising:

a) providing to a user a key rotation element and a key (K_i), wherein later versions of the key rotation element are determinable by the user but previous versions of the key rotation element are not determinable by said user;

b) generating a later version of the key (K_{i+n}) based on a later version of the key rotation element, wherein "n" is a positive integer;

c) providing to the user the later version of the key (K_{i+n}); and

d) said user determining a version of the key from ($K_i - K_{i+n-1}$), inclusive, by applying a version of the key rotation element to a version of the key from ($K_{i+1} - K_{i+n}$), inclusive.

9. The method of Claim 8, wherein said d) comprises:

d1) said user determining a later version of said key rotation element from said key rotation element provided in said a).

10. The method of Claim 9, wherein said d) further comprises:

d2) said user determining version of the key K_{i+n-1} by applying version of the key rotation element to the version of the key K_{i+n}.

11. The method of Claim 8, further comprising:

e1) generating new key rotation element;

e2) generating new key based, in part, on said new key rotation element; and

e3) distributing said key to non-revoked users.

12. The method of Claim 8, wherein said a) further comprises providing a secret share and a key rotation catalyst said user, wherein said secret share and said key rotation catalyst allow said user to generate a next key in the series provided sufficient public information is available.

13. The method of Claim 12, further comprising:

e) publishing at least one public share, wherein the next key in the series is determinable based on the key rotation catalyst, the secret share, and the at least one public share.

14. The method of Claim 12, further comprising revoking a user by publishing a version of the revoked user's secret share.

15. A method of windowed backward file key generation, comprising:

a) generating an initial file key;

b) generating an initial key rotation exponent, wherein said key rotation exponent allows previous versions of file keys to be determined back until a pre-determined version of the file key, but no file keys further back; and

c) providing said initial file key and said initial key rotation exponent to initial users.

16. The method of Claim 15, further comprising:

d) joining a new user by distributing said new file key and said new key rotation exponent to said user.

17. The method of Claim 15, further comprising:

d1) generating a new key rotation exponent;

d2) generating a new file key based, in part, on said new key rotation exponent; and

d3) distributing said new file key to non-revoked users.

18. The method of Claim 15, further comprising:

d) a user generating a previous version of the file key by applying a version of the key rotation exponent to a version of the file key.

19. The method of Claim 15, wherein:

said a) further comprises generating a key rotation catalyst; and

said c) further comprises providing a secret share and said key rotation catalyst to ones of said initial users, wherein said secret share and said key rotation catalyst allow said initial users to generate a new version of the file key provided sufficient public information is available.

20. The method of Claim 19, further comprising:

d) publishing a public share, wherein said initial users are able to determine a new version of the file key using their own secret shares, the public shares, the key rotation catalyst, and a previous file key.

21. The method of Claim 19, further comprising:

d1) generating a new key rotation catalyst;

d2) publishing said new key rotation catalyst;

d3) generating a new file key based, in part, on said new key rotation catalyst; and

d4) publishing a revoked user's private share.